Center for Unified Biometrics and Sensors
University at Buffalo The State University of New York

Securing Pervasive Networks Using Biometrics

Viraj S. Chavan, Sharat Chikkerur, Sergey Tulyakov and Venu Govindaraju
Center for Unified Biometrics and Sensors,
University at Buffalo
http://www.cubs.buffalo.edu

Abstract

- **Challenges in pervasive computing environments**
  - Computing devices are numerous and ubiquitous
  - Traditional authentication including login schemes do not work well with so many devices
- **Proposed Solution**
  - Use biometrics for authentication
  - At the same time, ensure security of biometric templates in an open environment
- **Contributions**
  - Propose a biometrics based framework for securing pervasive environment
  - Implemented a novel scheme for securing biometric data in an open environment using symmetric hash functions

Background

- "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it" – Mark Weiser
- Pervasive Computing
  - A web of computing devices and sensors embedded in everyday objects ranging from cars to house appliances
  - The devices are context sensitive and user 'aware'
  - Focus on human computer interaction and AI
  - Existing efforts
    - Project Oxygen , MIT [1]
    - Project Aura, CMU [2]
    - Planet Blue, IBM [3]

Aspects of a Pervasive Environment

- **User Interaction**
  - User interacts with speech, gestures and movements
  - The sensors and computing devices are 'aware' of the user and in the ideal case are also aware of his 'intent'.
- **Proactivity**
  - The computing devices should interact and query other devices on Transparency
- **Technology has to be transparent.**
  - behalf of the user and his intent
- **Device interaction**
  - Frequent Multiparty interactions
  - No central authority or third party

Security and Privacy

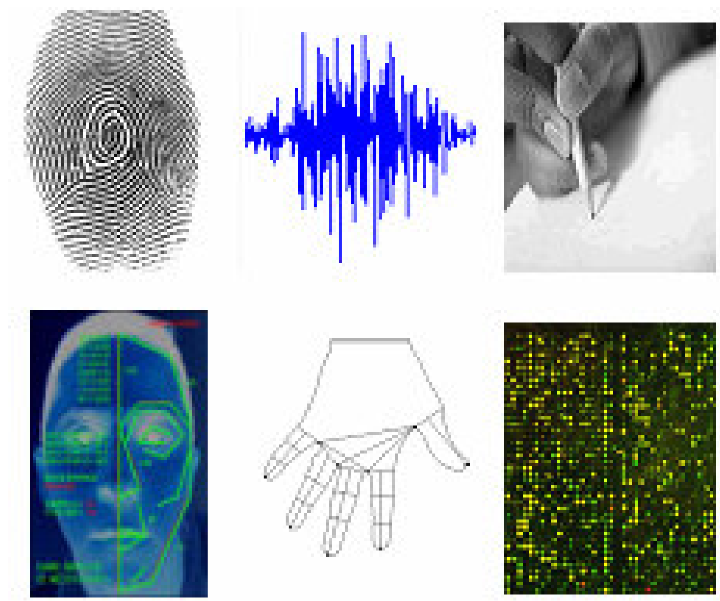
- **Consequences of a pervasive network**
  - Devices are numerous, ubiquitous and shared
  - The network shares the context and preferences of the user
  - Smart spaces are aware of the location and intent of the user
- **Security Concerns**
  - Only authorized individuals need to be given access
  - Authentication should be minimally intrusive
  - Devices should be trustworthy
- **Privacy issues**
  - User should be aware of when he is being observed
  - The user context should be protected within the network
- Need to balance accessibility and security
- Should be scalable with multiple users operating in the network

Learn from History?

- **Wireless networks**
  - Initial research focused on implementing wireless and ad hoc networking devices and protocols
  - Security an afterthought?
- **Lessons for pervasive computing**
  - Human computer interface issues will be solved eventually
  - Network infrastructure will mature
  - Security has to be considered in the design stage
- **Foresights**
  - Authentication has to be transparent
  - Trusted third party may not be available
  - Traditional key based systems will not scale well
  - Trust based models work well with devices and agents
  - Trust is not well defined for human user

Solution: Biometrics?

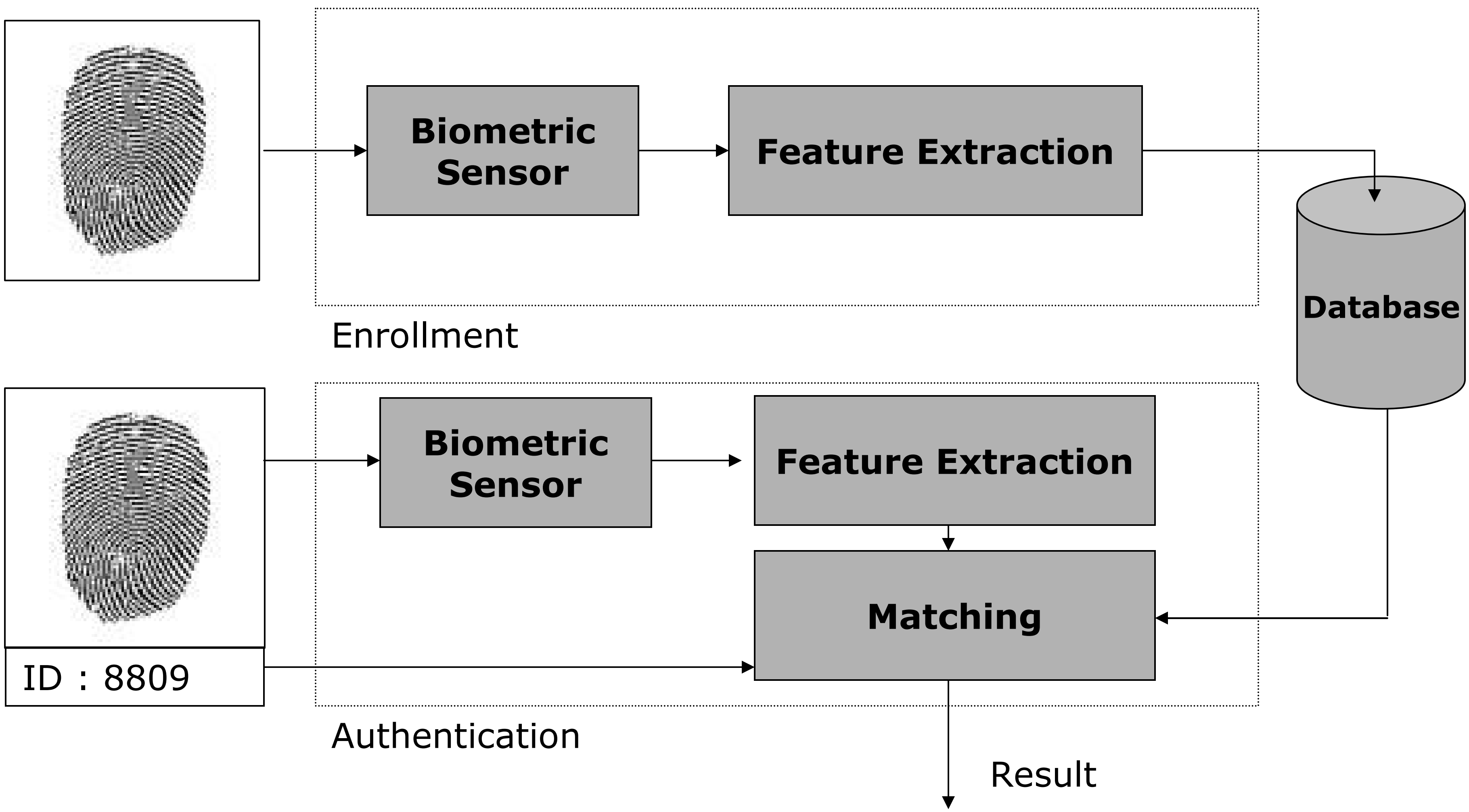
- **Definition**
  - Biometrics is the science of verifying and establishing the identity of an individual through physiological features or behavioral traits.
- **Examples**
  - Physical Biometrics
    - Fingerprint
    - Hand Geometry
    - Iris patterns
  - Behavioral Biometrics
    - Handwriting
    - Signature
    - Speech
    - Gait
  - Chemical/Biological Biometrics
    - Perspiration
    - Skin composition(spectroscopy)



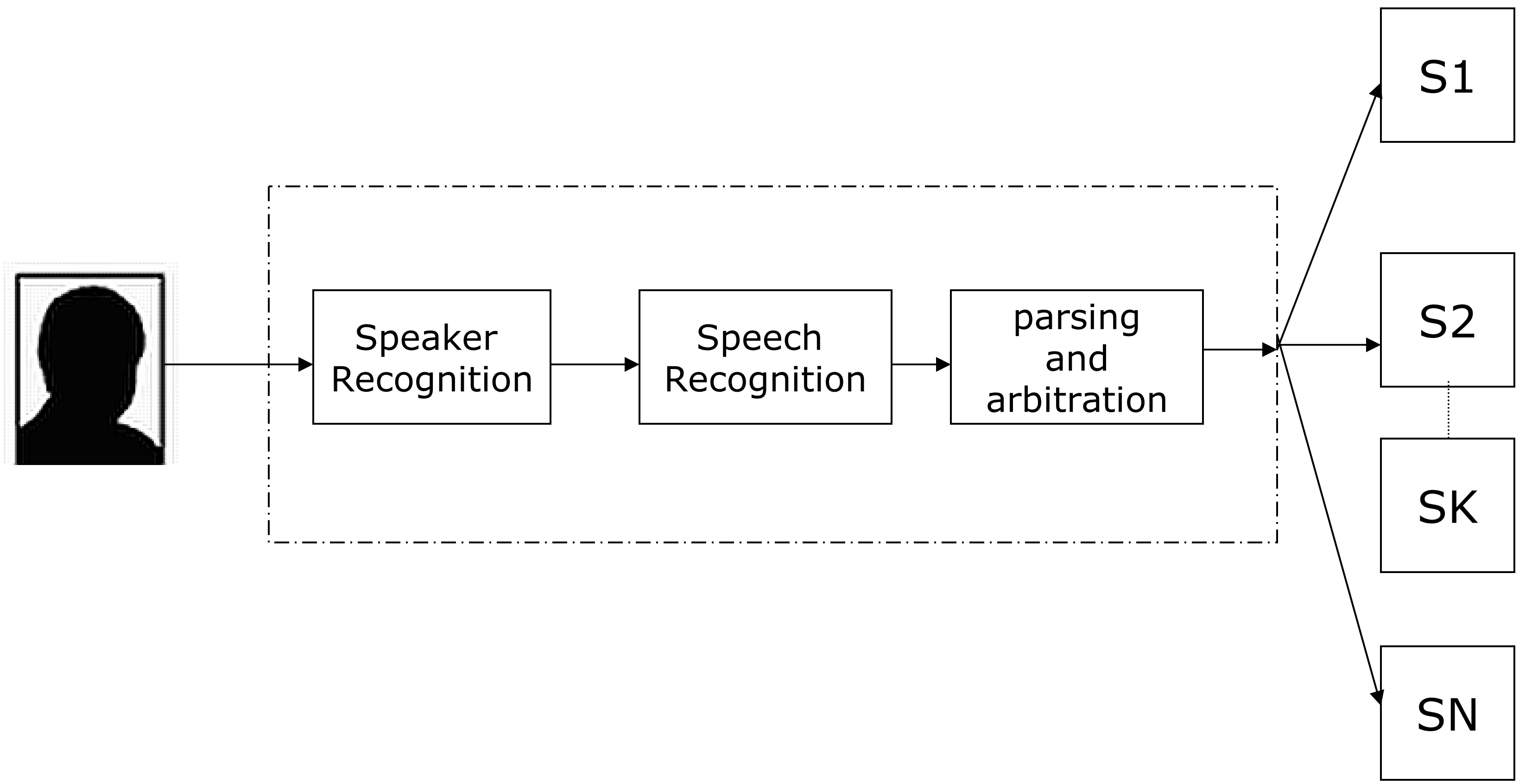
Why Biometrics?

- With numerous devices, traditional paradigm of user name and password based scenarios are not practical
- Only authorized users should have access to data and services
- Biometrics provide an unobtrusive and convenient authentication mechanism
- Advantages of biometrics
  - Uniqueness
  - No need to remember passwords or carry tokens
  - Biometrics cannot be lost, stolen or forgotten
  - More secure than a long password
  - Solves repudiation problem
  - Not susceptible to traditional dictionary attacks

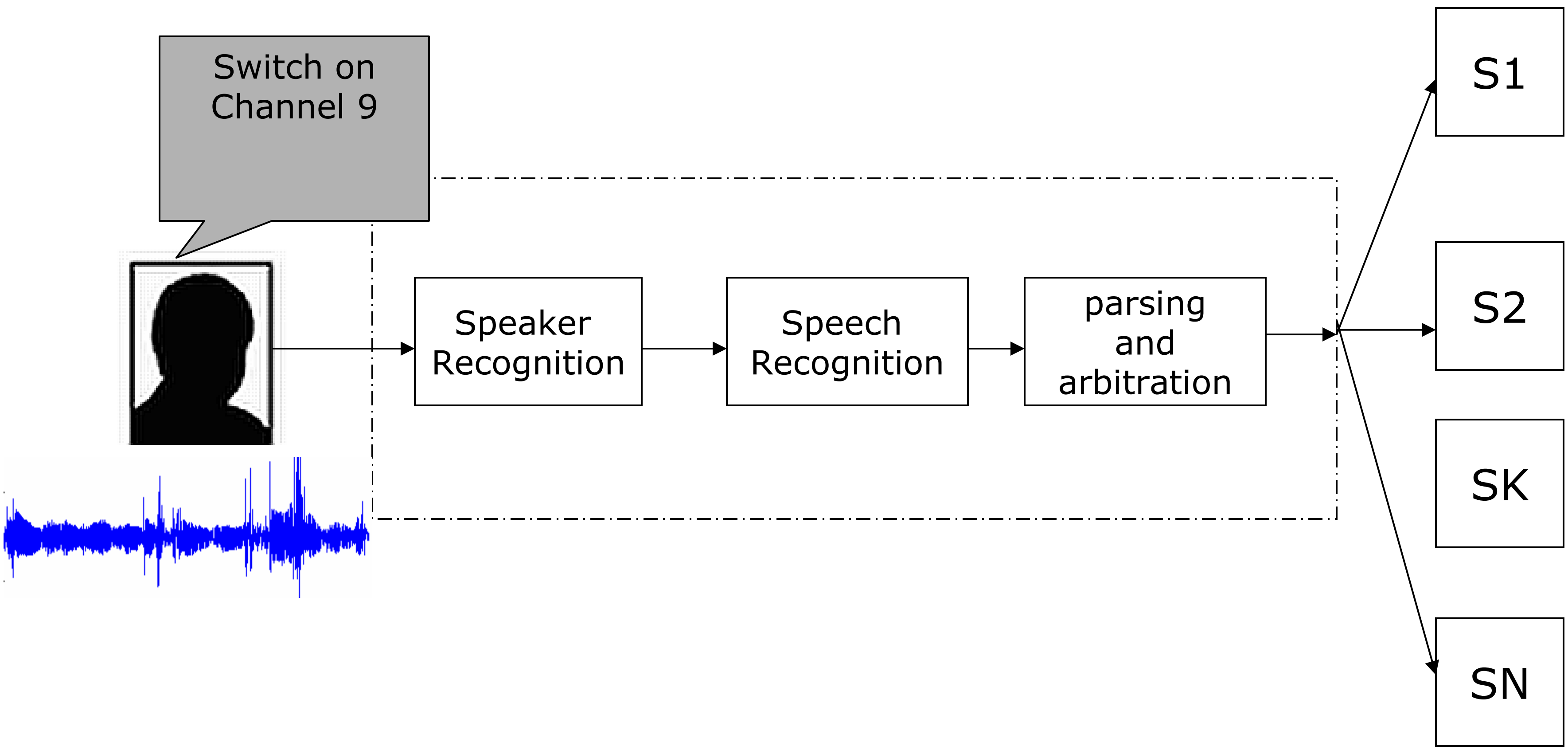
General Biometric System



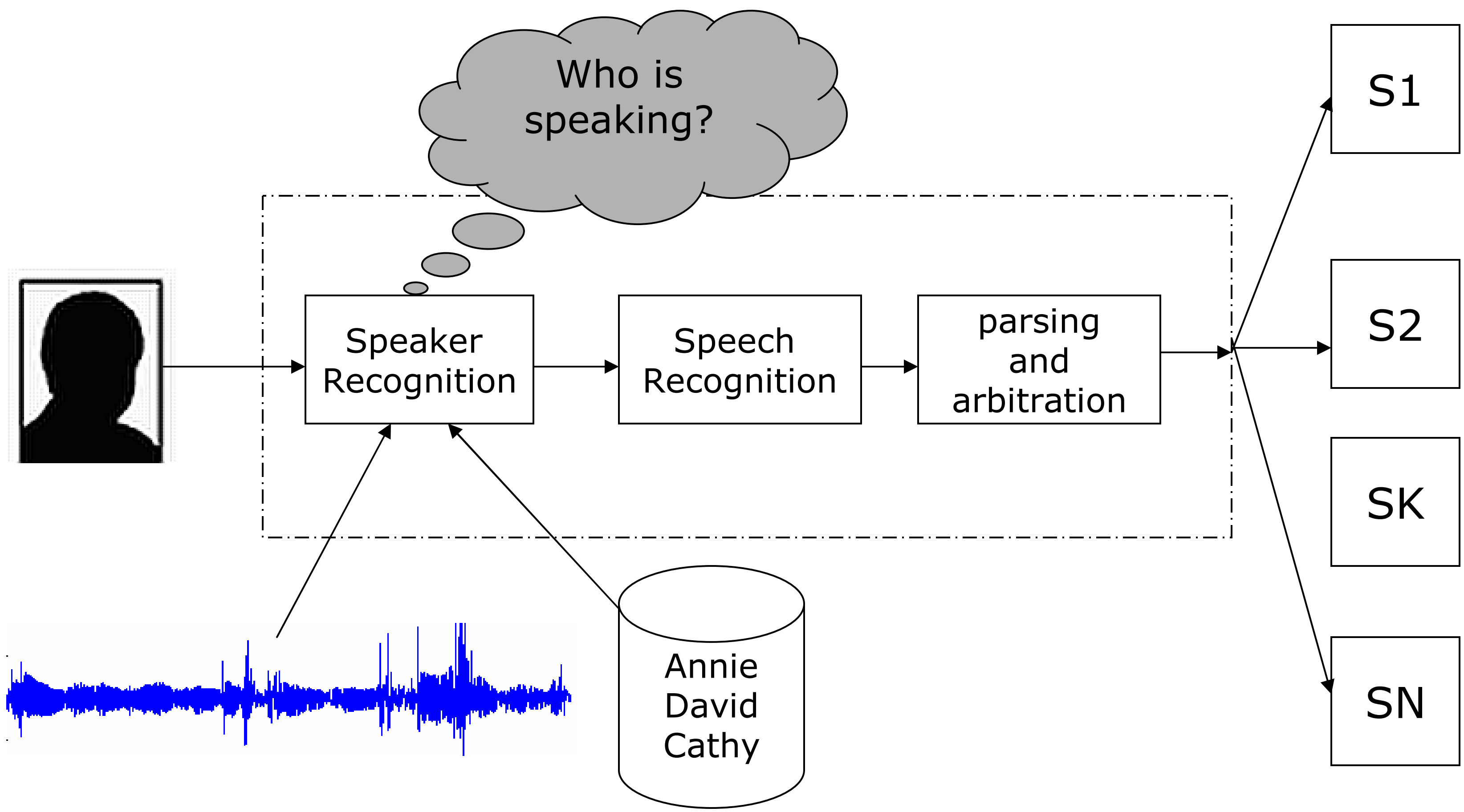
Framework for Authentication/Interaction



Framework for Authentication/Interaction

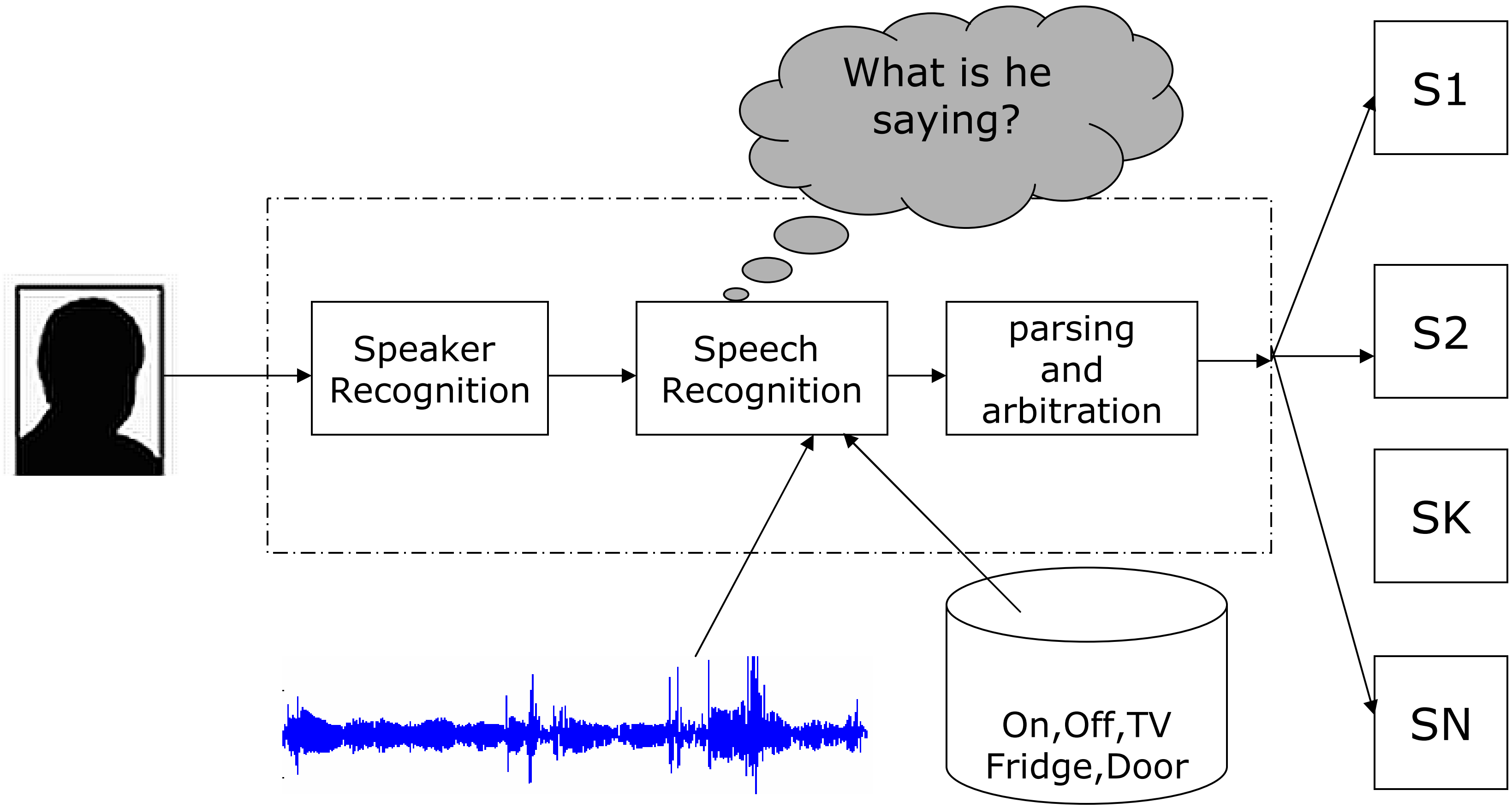


Framework for Authentication/Interaction



"Authentication"

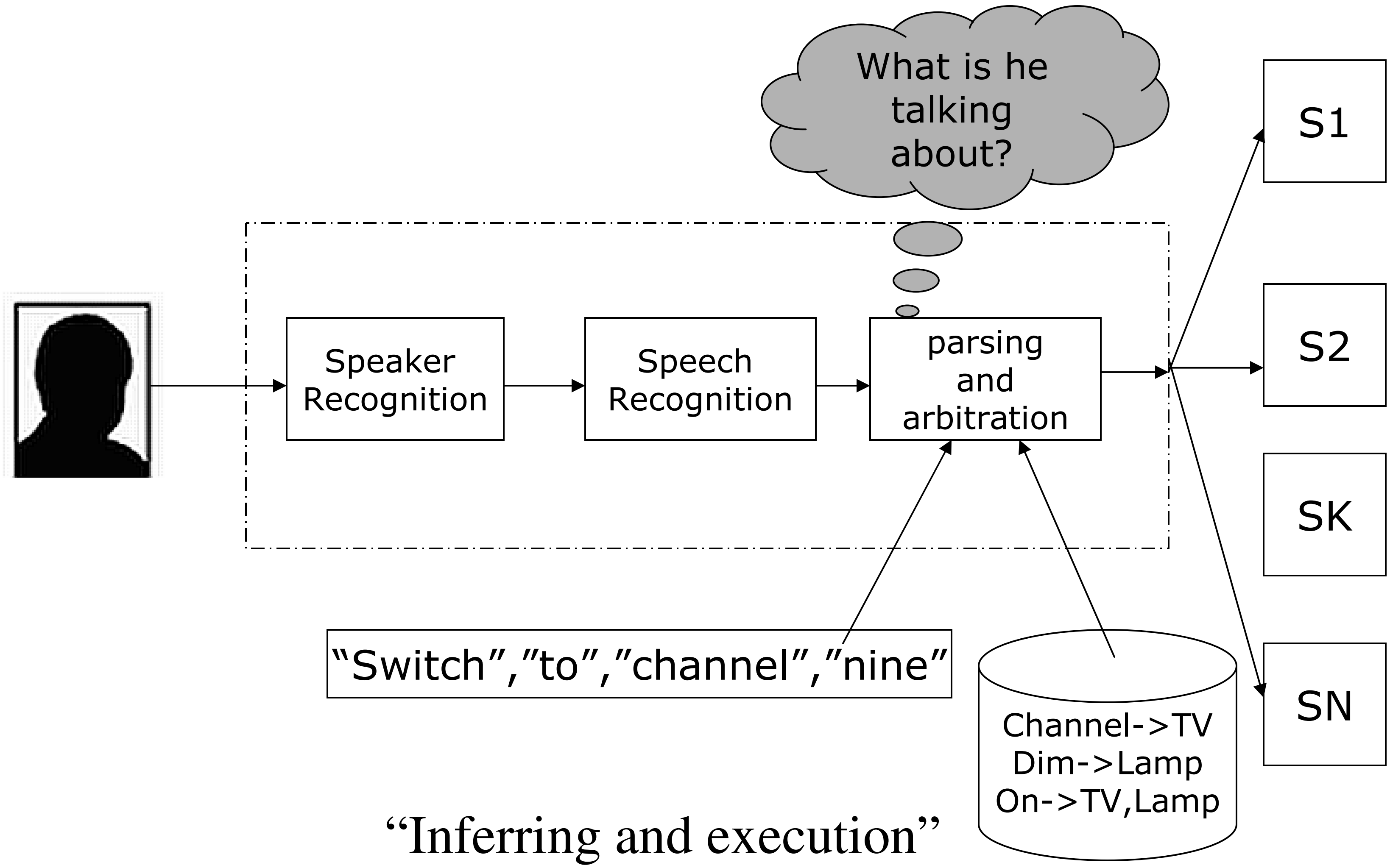
Framework for Authentication/Interaction



"Understanding"

Center for Unified Biometrics and Sensors
University at Buffalo The State University of New York

Framework for Authentication/Interaction

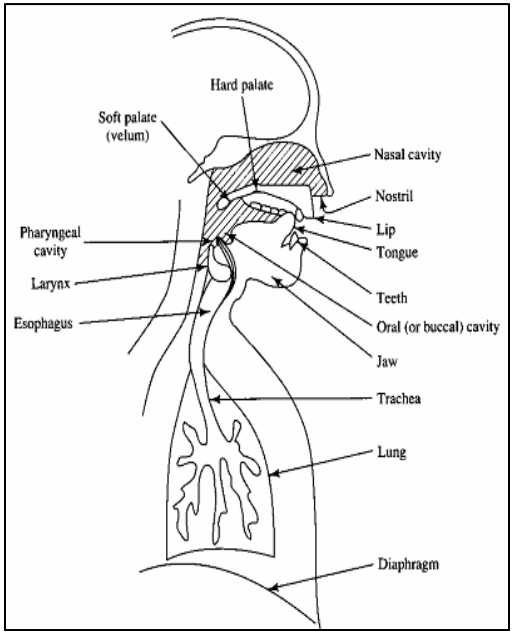


"Inferring and execution"

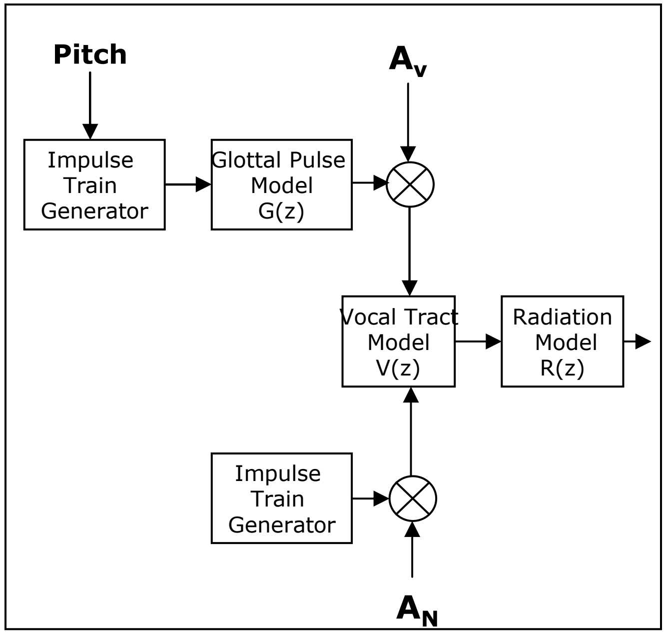
Speaker Recognition

- **Definition**
  - It is the method of recognizing a person based on his voice
  - It is one of the forms of biometric identification
- **Depends of speaker specific characteristics.**

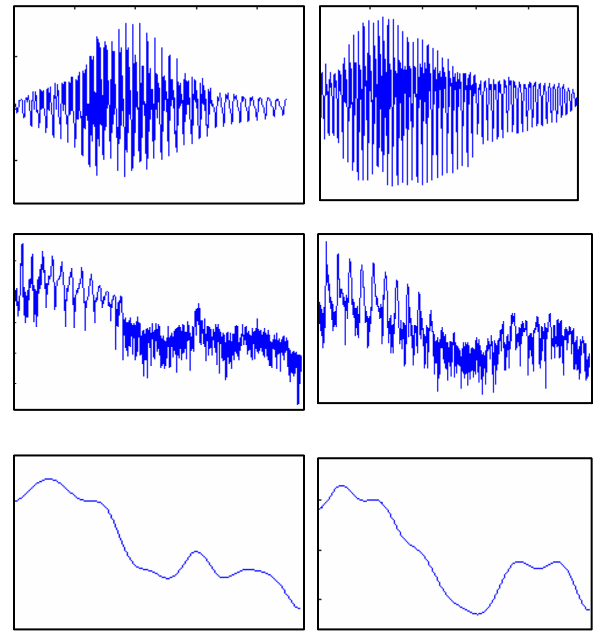
Speaker Recognition



Speech Production Mechanism

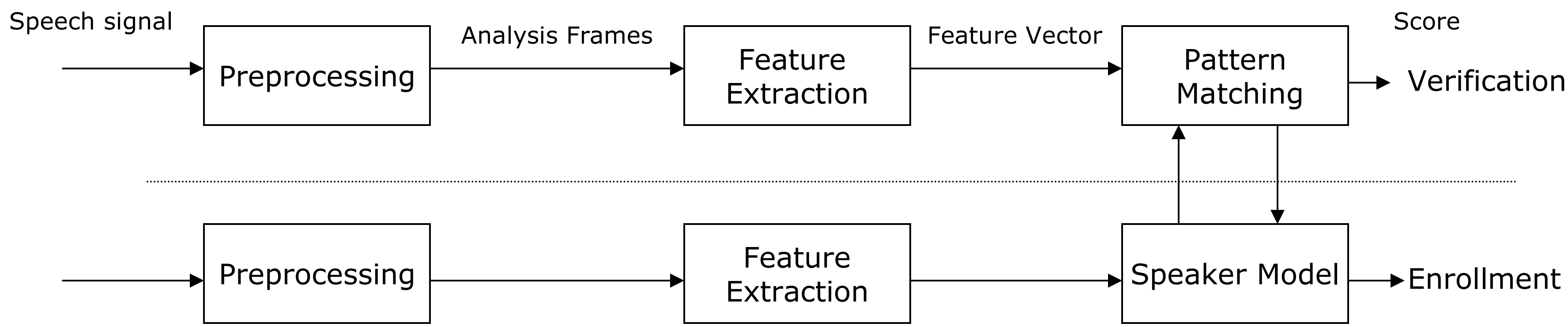


Speech production Model



Vocal Tract Modeling

Generic Speaker Recognition System



- A/D Conversion
- End point detection
- Pre-emphasis filter
- Segmentation

- LAR
- Cepstrum
- LPCC
- MFCC

- Stochastic Models
  - GMM
  - HMM
- Template Models
  - DTW
  - Distance Measures

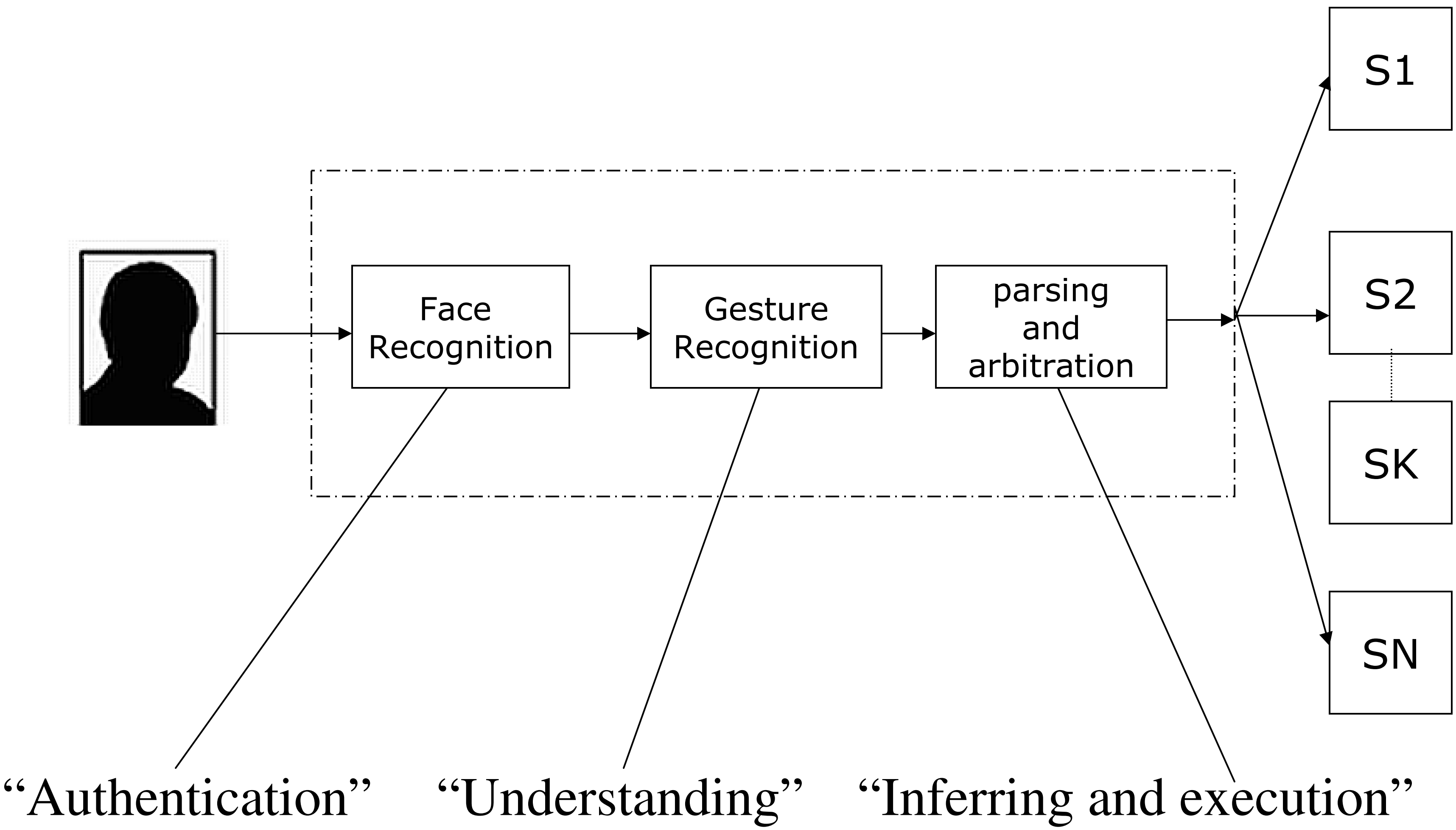
- **Choice of features**
  - Differentiating factors b/w speakers include vocal tract shape and behavioral traits
  - Features should have high inter-speaker and low intra speaker variation

State of the art in speech

- **Literature**
  - 0.3%, Colombi et al. (Cepstrum)
  - 6-8%, Reynolds(MelCepstrum)
  - 4% Wan and Renals, (SVM)
- **NIST Speaker Recognition evaluation**
  - ~1% FAR, 10-15% FRR (Text independent)
- **Via voice**
  - IBM voice recognition engine is being open sourced
- **'Speech recognition on a chip'**
  - CMU is developing a chip architecture to completely embed speech recognition on a single chip

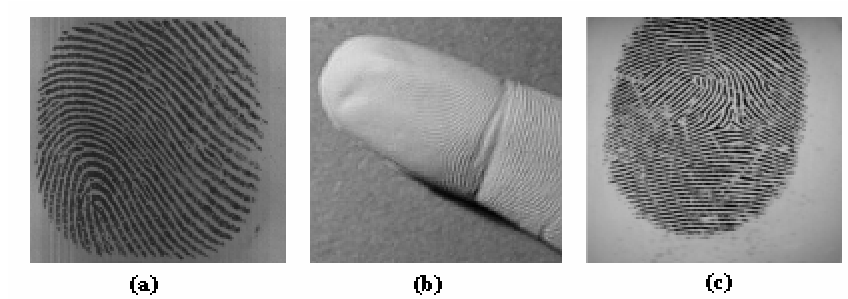
Center for Unified Biometrics and Sensors
University at Buffalo The State University of New York

Framework is Generic



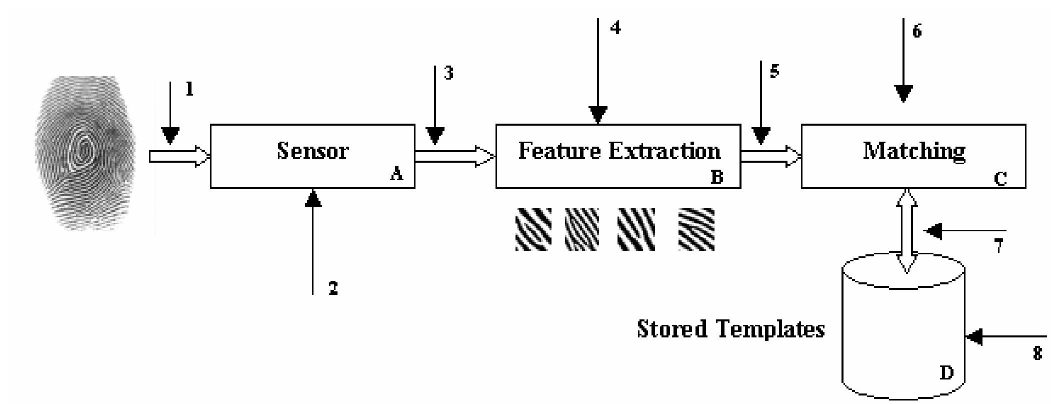
Security of Biometric Data

- **Issues in biometrics**
  - Biometrics is secure but not secret
  - Permanently associated with user
  - Used across multiple applications
  - Can be covertly captured



Fake Biometrics

- **Types of circumvention**
  - Denial of service attacks(1)
  - Fake biometrics attack(2)
  - Replay and Spoof attacks(3,5)
  - Trojan horse attacks(4,6,7)
  - Back end attacks(8)
  - Collusion
  - Coercion

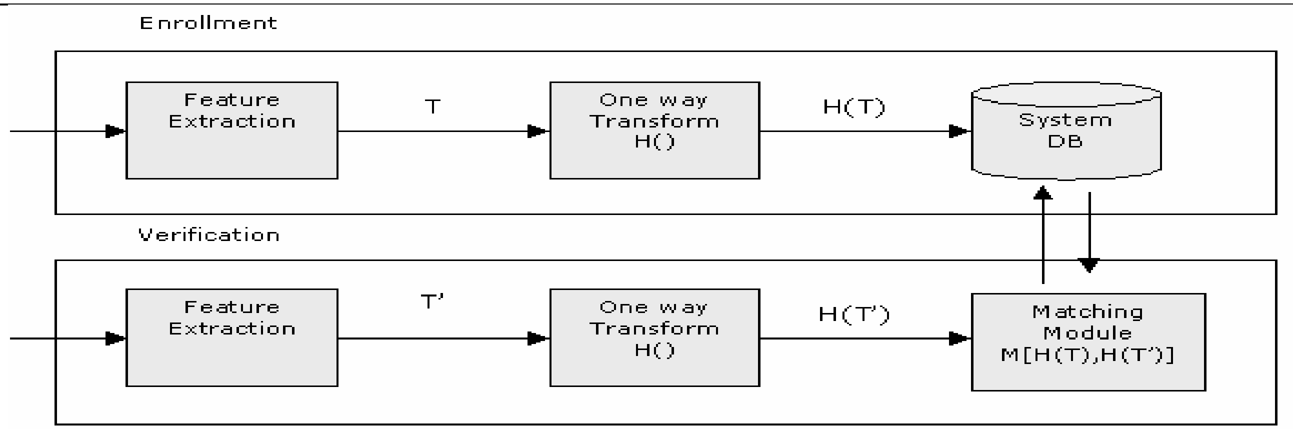


Threats to a Biometric System

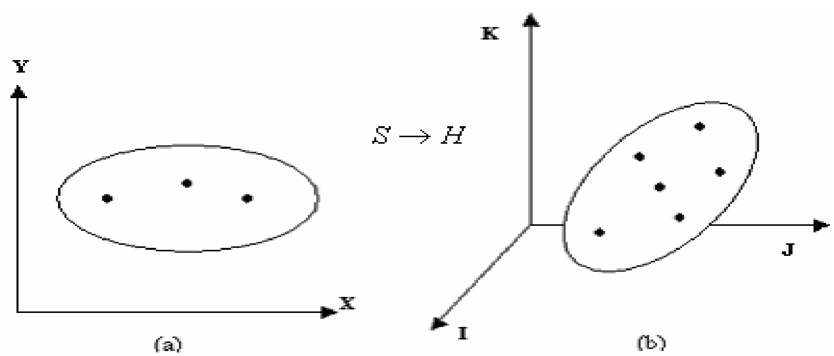
Hashing

- **Hashing**
  - Instead of storing the original password P, a hashed values P'=H(P) is stored instead.
  - The user is authenticated if H(password) = P'.
  - It is computationally hard to recover P given H(P)
  - H() – one way hashing function
- **Problem with biometrics**
  - Biometric data has high uncertainty
  - Matching is inexact/probabilistic
  - Therefore, hashing function should be error tolerant

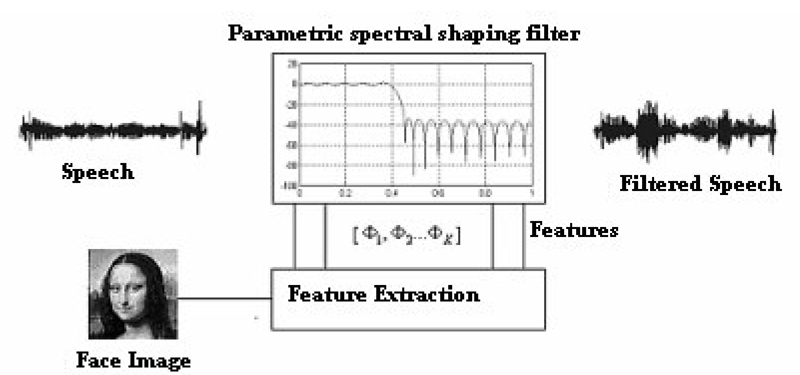
Biometric Hashing



Hashing Schema

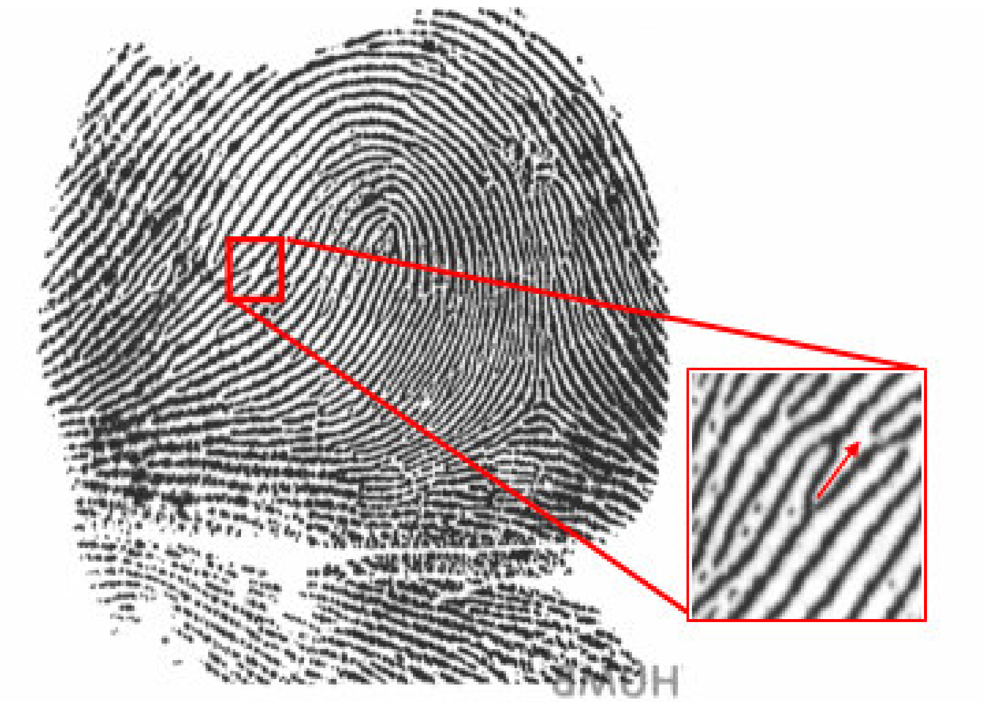


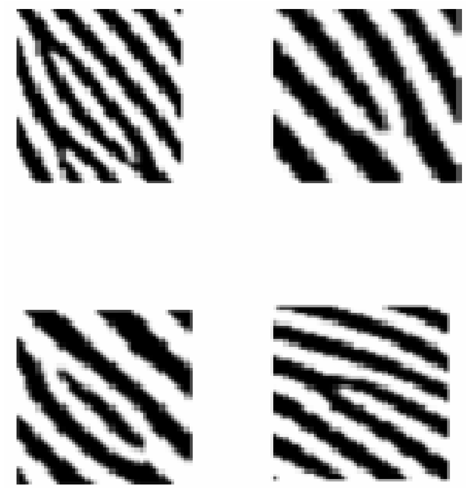
Hashing



Personalized Hashing

Fingerprints 101

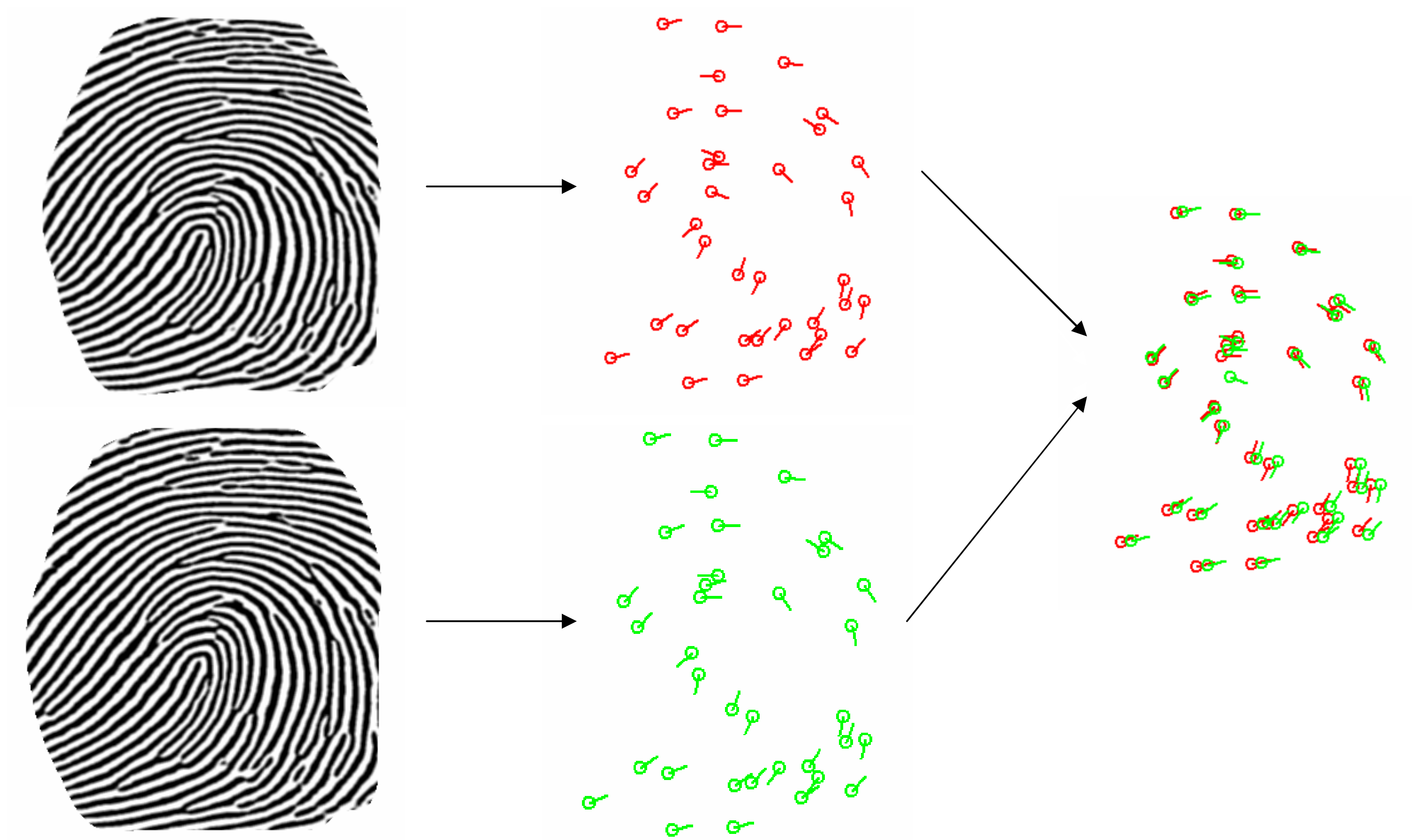




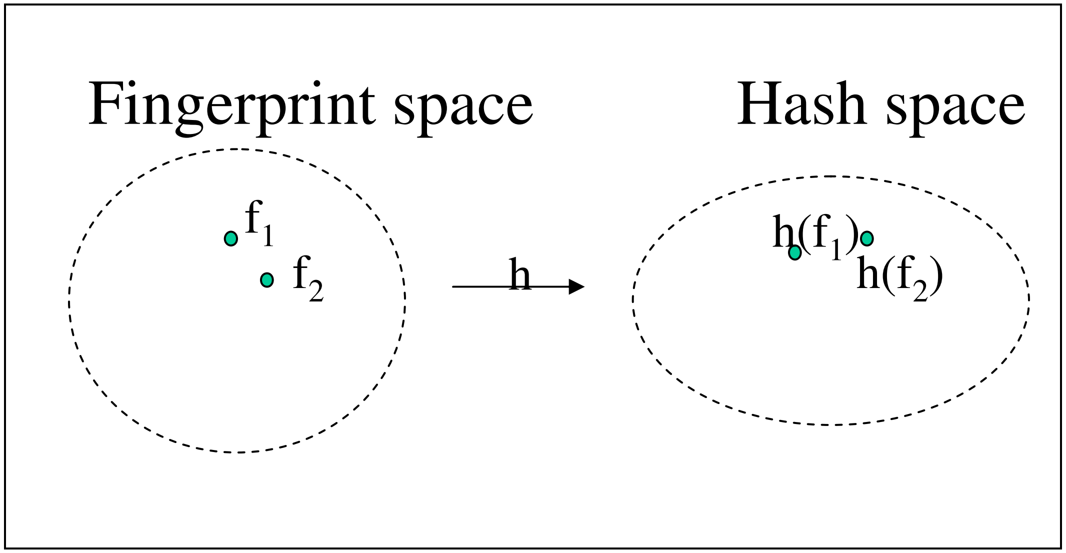
X	Y	θ	T
106	26	320	R
153	50	335	R
255	81	215	B

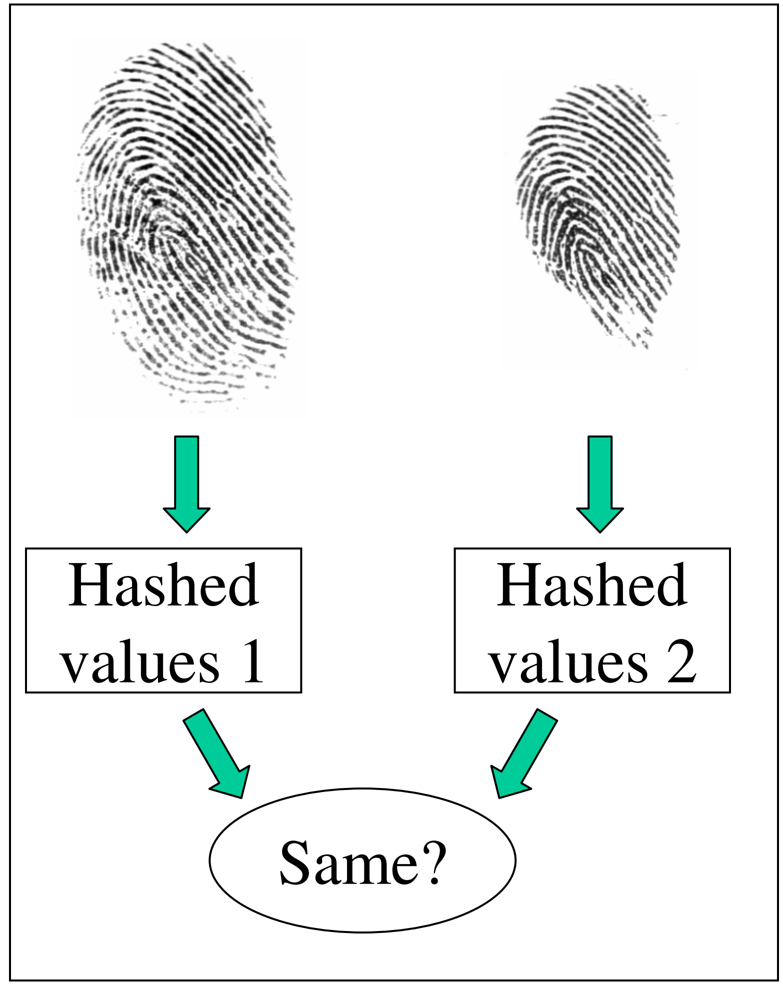
- **Minutiae: Local anomalies in the ridge flow**
- **Pattern of minutiae are unique to each individual**

Fingerprint Verification



Research Challenges





- Images include different scanned area.
- Set of features is different for two different fingerprints of the same finger.
- Similar fingerprints should have similar hash values
- Hash values should be invariant to rotation/translation

Hash functions of minutia points

Consider following functions of minutia positions:

$$h_1(c_1, c_2, \ldots, c_n) = c_1 + c_2 + \ldots + c_n$$

$$h_2(c_1, c_2, \ldots, c_n) = c_1^{\,2} + c_2^{\,2} + \ldots + c_n^{\,2}$$

$$\vdots$$

$$h_m(c_1, c_2, \ldots, c_n) = c_1^{\,m} + c_2^{\,m} + \ldots + c_n^{\,m}$$

The values of these symmetric functions do not depend on the order of minutia points.

Hash functions of transformed minutiae

What happens with hash functions if minutia point set is transformed?

$$h_1(c_1', c_2', \ldots, c_n') = c_1' + c_2' + \ldots + c_n'$$
$$= (rc_1 + t) + (rc_2 + t) + \ldots + (rc_n + t)$$
$$= r(c_1 + c_2 + \ldots + c_n) + nt = rh_1(c_1, c_2, \ldots, c_n) + nt$$

$$h_2(c_1', c_2', \ldots, c_n') = c_1'^2 + c_2'^2 + \ldots + c_n'^2$$
$$= (rc_1 + t)^2 + (rc_2 + t)^2 + \ldots + (rc_n + t)^2$$
$$= r^2(c_1^2 + c_2^2 + \ldots + c_n^2) + 2rt(c_1 + c_2 + \ldots + c_n) + nt^2$$
$$= r^2 h_2(c_1, c_2, \ldots, c_n) + 2rth_1(c_1, c_2, \ldots, c_n) + nt^2$$

Symmetric Hash Functions

- n=2, m=1: for each minutia point we find it nearest neighbor, and

$$h_1(c_1, c_2) = \frac{c_1 + c_2}{2}$$

- n=3, m=1: for each minutia point we find two nearest neighbors and

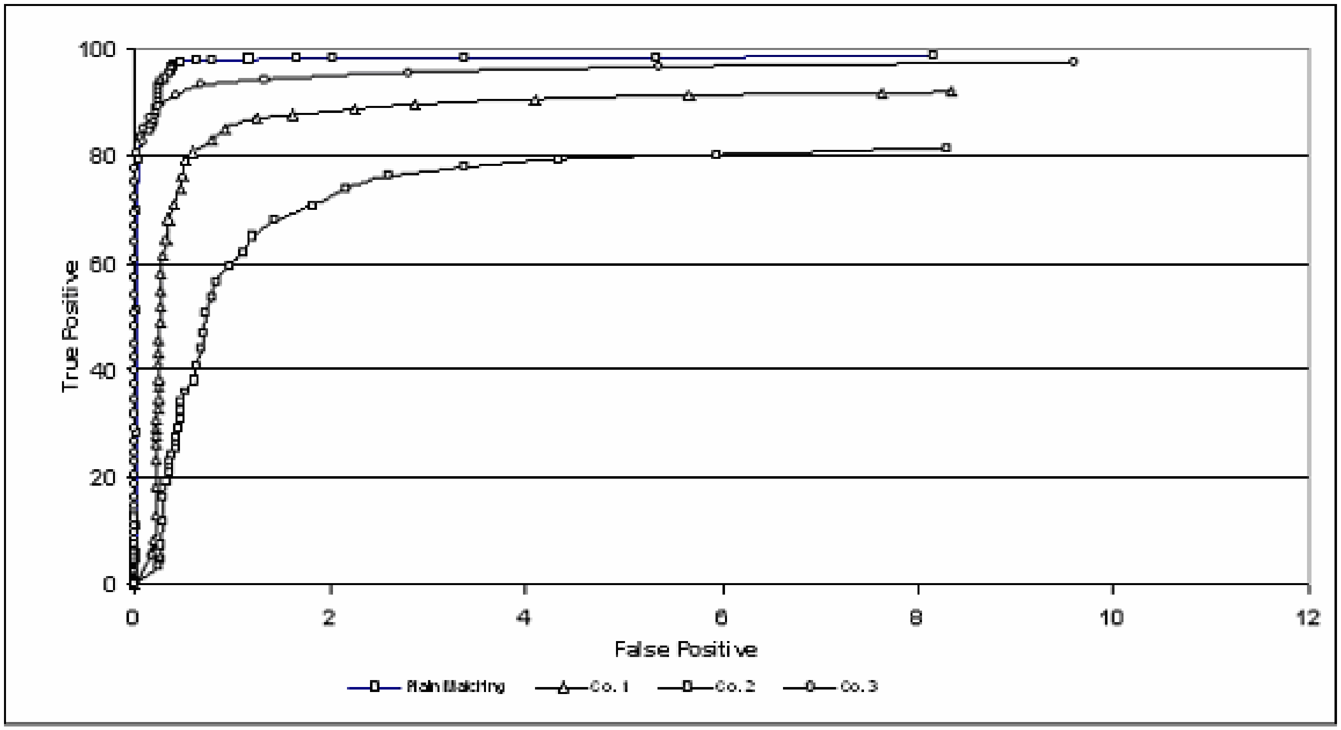
$$h1(c_1, c_2, c_3) = \frac{(c_1 + c_2 + c_3)}{3}$$

- n=3, m=2: for each minutia point find three nearest neighbors, and for each minutia triplet including original minutia point construct 2 hash functions

$$h1(c_1, c_2, c_3) = \frac{(c_1 + c_2 + c_3)}{3}$$

$$h_2(c_1, c_2, c_3) = \frac{(c_1 - h_1)^2 + (c_2 - h_2)^2 + (c_3 - h_3)^2}{3}$$

Results



- We used fingerprint database of FVC2002 with 2800 genuine tests and 4950 impostor tests
- We obtained a best result of Total Error Rate of 4.5% as compared to a Total Error Rate of 2.5% for plain minutia-based matching
- Acceptable verification rates allowing for encryption of fingerprint minutia data

Conclusion

- Smart spaces and pervasive computing are moving from concepts to implementations
- Security has to be incorporated in the design stage
- Traditional authentication and access control paradigms cannot scale to numerous and ubiquitous devices
- Biometrics serves as a reliable alternative for minimally intrusive authentication
- Biometrics solves key management and repudiation problem
- Securing biometrics is a major challenge in an open environment
- Biometric hashing can be used to create revocable biometric templates

Thank You

http://www.cubs.buffalo.edu

Implementations of Pervasive Computing

1. MIT Project Oxygen. http://oxygen.lcs.mit.edu/videometaglue.html
2. CMU Project Aura. http://www-2.cs.cmu.edu/ aura/.
3. IBM Planet Blue, http://researchweb.watson.ibm.com/compsci/planetblue.html